**AMENDMENTS TO THE SPECIFICATION:**

Please insert the following paragraph and heading on page 1, between the title and first paragraph:

This disclosure is based upon French Application No. 02/04117, filed April 3, 2002, and International Appln. No. PCT/FR03/01058, filed April 3, 2003, the contents of which are incorporated herein.

Background of the Invention

Delete the partial sentence appearing on page 4, lines 1-2, and substitute the following paragraphs:

An instruction is said to be fictional if its execution does not modify the data manipulated by the algorithm. For example, the instruction i <- i – 0 is a fictional instruction (i is here a loop variable and the notation "<-" signifies incrementation, by zero here, of the loop variable).

Though this solution is effective against "timing attacks", it is not effective against other types of covert channel attack and it may also be detrimental to the algorithm execution time.

The most widely known covert channel attacks are the so-called simple or differential ones. Covert channel attack means an attack based on a physical quantity measurable from outside the device and whose direct analysis (simple attack) or analysis according to a statistical method (differential attack) makes it possible to discover information manipulated in processings carried out in the device. For example, in a "timing attack", the covert channel (the physical quantity measurable from the outside) is time.

Covert channel attacks can make it possible to discover confidential information. These attacks were in particular revealed by Paul Kocher (Advances in Cryptology - CRYPTO'99, Vol. 1666 of Lecture Notes in Computer Science, pp.388-397, Springer-Verlag, 1999).

Amongst the physical quantities which can be exploited for these purposes, there can be cited the execution time, the current consumption, the electromagnetic field radiated by the part of the component used for executing the calculation, etc. These attacks are based on the fact that, during the execution of an algorithm, the manipulation of a bit, that is to say its processing by a particular instruction, leaves a particular imprint on the physical quantity in question, according to the value of this bit and/or according to the instruction.

Please insert the following heading on page 6, between lines 5 and 6:

Summary of the Invention

Please insert the following heading on page 13, between lines 4 and 5:

Brief Description of the Drawings

Please insert the following heading on page 13, between lines 18 and 19:

Detailed Description